

UNITED STATES DISTRICT COURT

for the
Southern District of Texas

United States Courts
Southern District of Texas
FILED

JUN 11 2018

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No.

David J. Bradley, Clerk of Court

G - 18 - 039

information associated with user ID: 912419232 and/or
email account: malikberlanga2@gmail.com that is stored
at premises controlled by Dropbox, Inc.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
2251(a), 2252(a) et seq.	Possession, Receipt, Distribution of Child Pornography

The application is based on these facts:

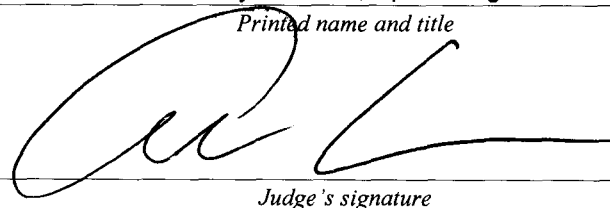
- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

DeWayne Lewis, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: June 11, 2018


Judge's signature

City and state: Galveston, Texas

Andrew M. Edison, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
USER ID 912419232 AND/OR EMAIL
ACCOUNT malikberlanga2@gmail.com
THAT IS STORED AT PREMISES
CONTROLLED BY DROPBOX, INC.

Case No. **G - 18 - 039**

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, DeWayne Lewis, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., a company headquartered at 333 Brannon Street, San Francisco, California 94107. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox, Inc. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, a government-authorized person will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), assigned to the Homeland Security Investigations (HSI) office in Galveston, Texas. I have been so employed since June 2002. As part of my duties as an ICE agent, I investigate criminal violations related to child exploitation and child pornography, including

violations pertaining to online extortion and/or stalking, adults attempting to meet with juveniles for sexual encounters and the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A . I have received training in the area of child pornography and child exploitation, and I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256)¹ in all forms of media, including computer media. I have participated in the execution of numerous search warrants and covert operations involving child exploitation and the online solicitation of minors, many of which involved child exploitation and/or child pornography offenses. I am in routine contact with experts in the field of computers, computer forensics, and Internet investigations. I annually attend the Dallas Crimes Against Children Conference where I attain various investigative training. I am currently a member of the Houston Metro Internet Crimes Against Children Task Force. This task force includes prosecutors and members of multiple police agencies across the southeast/coastal Texas and Houston metro regions.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), et seq., which make it a crime to possess child pornography, violations of Title 18 U.S.C. §§

¹ “Child Pornography means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . [or] (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.” For conduct occurring after April 30, 2003, the definition also includes “(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct,” 18 U.S.C. § 2256(8).

2252(a)(2) and 2252A(a)(2), et seq., which make it a crime to receive/distribute child pornography in interstate commerce by computer, and violations of 18 U.S.C. §§ 2252(a)(1) and 2252A(a)(1), et seq., which make it a crime to transport or ship child pornography in interstate commerce have been committed by Malik Berlanga. There is also probable cause to search the information described in Attachment A for evidence, contraband, instrumentalities and/or fruits of these crimes, as described in Attachment B.

DROPBOX

5. Dropbox is a service that allows its users to store files on Dropbox's servers. According to the Dropbox privacy policy, Dropbox collects and stores files that are uploaded, downloaded, or accessed with the Dropbox service. Dropbox also collects logs, which includes information from the customer's device, its software, and customer activity using the Dropbox services. That information can include the customer's device's Internet Protocol ("IP") address, browser type, the web page the customer visited before he went to the Dropbox website, information searched for on the DropBox website, locale preferences, identification numbers associated with the customer's devices, their mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning a customer's files, and other interactions with the Drobox services. Dropbox is a free service that allows customers to bring all their files, photos, documents, and videos anywhere. That means that any file a customer saves to their Dropbox account will automatically save to all of the customer's computers, phones and even the Dropbox website.

PROBABLE CAUSE

6. The Houston Metro Internet Crimes Against Children (ICAC) task force received information about suspicious activity from a cloud service company named Dropbox, Inc. Dropbox reported to the National Center for Missing and Exploited Children (NCMEC) on August 18, 2017, that someone was using their cloud services to store or transfer suspicious images of nude minors via the internet. Dropbox viewed 10 files that were publicly available and provided those images to NCMEC. The report was forwarded to the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI) Resident Agent in Charge office in Galveston, Texas. HSI Special Agent DeWayne Lewis received and reviewed the report. There were approximately 10 suspicious files that consisted of videos depicting nude minor females exposing their genitals and engaging in sexual activity. The Dropbox customer information associated with the account was, in part:

Email Address:	malikberlanga@gmail.com
Screen/User name:	Angry Lemon
User ID:	624294467
IP Address:	108.236.175.167 (Login) 05-30-2017 06:03:51 UTC

7. The IP address, 108.236.175.167, was one managed by the internet service provider AT&T. Officer Wendy Corrales, a police officer with the Houston Police Department, and member of the Houston Metro ICAC, had a subpoena issued to AT&T on September 7, 2017, for subscriber information about the customer assigned IP address 108.236.175.167 on May 30, 2017, at 06:03:51 UTC. AT&T responded to her subpoena on/about September 9, 2017, with the following information, in part:

Address: 315 WESTWOOD
FRIENDSWOOD TX 77546

8. Special Agent Lewis examined the cache of suspicious files that Dropbox viewed and reported to NCMEC from Malik Berlanga's Dropbox activity. The following two examples fit the federal definition of child pornography and are from that collection of files:

Title: IMG_3090.mp4 was a color video which had a production title on the screen introducing it as "Preschool Baby Sluts." It depicted a compilation of short video clips of different nude Caucasian minor females, ranging in age from approximately two to five years old, performing oral sex on different adult Caucasian males' erect penises, some of the adults performing oral sex on the minors and some of the adults penetrating the minors' vaginas and anuses with their erect penises.

Title: IMG_4755.mp4 was a color video that depicted a nude 4-5 year old Caucasian minor female performing oral sex on a nude adult Caucasian male. The video continued as the minor paused while the adult masturbated in front of her face until he ejaculated on her chest and face.

9. Special Agent Lewis had a federal search warrant served on Dropbox, Inc. on October 6, 2017, for Berlanga's collection of stored content, log files and subscriber information. Dropbox provided the data on October 18, 2017. It contained the following titled folders and file structure, including a folder with the acronym "CP" in it, which is the common abbreviation for 'child pornography,' in part:

Maya

Personal CP

- Vids
- Yaneli

10. On March 13, 2018, HSI Galveston, the Houston Metro Internet Crimes Against Children task force and the Pearland Police Department executed a search warrant at 315 Westwood Drive in Friendswood, Texas. Special Agent Lewis and Pearland Police Department Detective Cecil Arnold asked to speak with Berlanga privately, and, although he was not in custody, read him the *Miranda* warnings, which he stated that he understood and agreed to participate in a voluntary

interview. Berlanga stated that he received and distributed child pornography through links via Instagram and Dropbox. Berlanga stated that the name "Yaneli" referred to his younger, 8-9 year old female cousin. Berlanga also explained that he had a foot fetish and had produced a video of himself licking the minor female cousin's feet and rubbing his penis on them. Berlanga explained that his previous Dropbox account had "died," but he had been using his newest one and downloaded a link containing child pornography as recently as two nights ago. Berlanga provided his alternate email address, malikberlanga2@gmail.com, associated with his new Dropbox account.

11. On May 3, 2018, Special Agent Lewis had a summons issued to Dropbox, Inc. for subscriber information regarding the customer using email address malikberlanga2@gmail.com. The customer information Dropbox provided on May 18, 2018, in response to the summons was, in part:

Name:	Angry Lemon
Email:	malikberlanga2@gmail.com
User ID:	912419232

CHARACTERISTICS COMMON TO INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

12. Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the sexual exploitation of children which includes the distribution, receipt, possession and collection of child pornography:

13. Individuals with a sexual interest in children receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

14. Individuals with a sexual interest in children collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals with a sexual interest in children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower, or “groom,” the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

15. Individuals with a sexual interest in children almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home, email account or in “virtual” storage, like in the iCloud or Dropbox.com. Individuals with a sexual interest in children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

16. “Child erotica,” as used in this Affidavit, is defined as materials or items that are sexually arousing to certain individuals but which are not in and of themselves obscene or do not necessarily depict minors in sexually explicit poses or positions. Such material may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.

17. Likewise, Individuals with a sexual interest in children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area or “virtual” storage. These collections are often maintained for several years and are kept close by, or remotely accessible, usually at, or via, the collector’s residence, to enable the collector to view his collection, which is highly valued.

18. Individuals with a sexual interest in children also may correspond with and/or meet

others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in sex with children or child pornography.

19. Individuals with a sexual interest in children prefer not to be without their child pornography, or prohibited from its' access, for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

20. Individuals with a sexual interest in children often have had, or continue to maintain, multiple email and social media accounts. It is common for such individuals to control multiple email addresses in their attempts to remain anonymous or thwart law enforcement's efforts to investigate their illicit activity. Some individuals will create an account to imply that they are of a different age or sex depending on what their online intentions are, or to pose as a person a potential victim already knows. Some individuals with a sexual interest in children will open multiple accounts, whether they be for email, social media or remote storage, with common denominators that can be identified by the host company that operates that medium. For example, a person with a sexual interest in children may create and maintain several different email accounts, but use the same email address as a "recovery" or "verifier" email account. Those individuals will use the same technique for new social media, email or virtual storage accounts when their original ones are compromised or shut down.

21. Individuals with a sexual interest in children often maintain contact information from their trusted sources or like-minded individuals. They also block, cancel or "unfriend," contacts that they perceive pose a threat to their illegal activity or have not maintained good standing. For

example, another individual with a sexual interest in children, but preferred children of a different age range or ethnicity, might be blocked by the other. They may also block a person who threatens to contact a parent or the police about their online activity. Likewise, a victim of coercion, enticement and/or sexual exploitation may block a suspect who is attempting to further victimize them.

22. Based upon my training, knowledge and experience in investigations related to child exploitation and my conversations with other law enforcement officers who have engaged in numerous investigations involving child pornography and exploitation, I am aware that individuals who access paid subscription or free sites offering images and/or videos depicting child pornography do so for the purpose of downloading or saving these images to their hard drive or other storage media so that the images and videos can be added to their collection. I know that individuals involved in the distribution of child pornography also continue to obtain images of child pornography found elsewhere on the Internet such as newsgroups and websites, and via paid subscriptions, as well as their own “trophy photos” of sexual conquests involving the exploitation of children.

23. Additionally, based upon my training, knowledge and experience in investigations related to child exploitation and child pornography cases, I am aware that individuals who have a sexual interest in children will oftentimes have a collection of child pornography and will ask children to take and send naked images of the themselves that would constitute child pornography as well as child erotica.

24. Furthermore, based upon my training, knowledge and experience in investigations related to child exploitation and child pornography cases, I am aware that individuals who have a sexual interest in children will oftentimes utilize social media such as Yahoo! Messenger, KIK Messenger and Craigslist and other online services to meet and communicate with minors. Individuals with a sexual interest in children know that social media allows for seemingly

anonymous communication which they can then use to groom the minors and set up meetings in order to sexually exploit them.

COMPUTERS AND CHILD PORNOGRAPHY

25. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers and computer technology (including advances in smartphones, tablets and internet connectivity) have revolutionized the way in which children are exploited and how child pornography is produced, distributed, and utilized. Advancements in cellular telephone technology and mobile applications have furthered those revolutionary methods of exploitation.

26. Cellular telephones are routinely connected to computers to re-charge the batteries and synchronize the mobile telephone with their matching computer programs, or “applications,” on the computer. Cellular telephones are connected to the user’s computer to transfer, save or back-up files or to download files, programs or “applications” via the internet, as one would do for music or ring tones. Users connect their cellular telephones to their computer to save, or back-up, their content or upload those files via the internet to a virtual storage medium like the iCloud or Dropbox, which allow users to access that content from any device with internet access, including their mobile devices (cellular phones or tablets) or another computer. Users can also download programs to their computers that mimic, or operate as if they are using, applications on their cellular telephone. Some of those examples include “iPadian,” “Andy,” and “BlueStacks.” People with a sexual interest in children have embraced these technologies in their efforts to exploit children, conceal their true identities, misdirect investigators, hide evidence and communicate with others with the same interests.

27. Technologies for portable cellular telephones, their batteries, internet connectivity and quick-charge devices have also greatly advanced. Today's vehicles often advertise built-in options for internet connectivity. In early 2013, General Motors announced it would partner with AT&T to outfit most of its 2014 models with high-speed data connectivity, with those same options available from Chrysler, Audi and Ford. These portable devices are commonly stored and used in vehicles and derive their power from being plugged in to cigarette lighters or auxiliary power outlets. Other portable navigation devices, like the Garmin or TomTom, provide turn-by-turn directions to previously unknown locations when the user inputs the desired address or destination and are commonly kept or stored in the user's vehicle. Many modern vehicles are equipped with satellite navigation from the factory. Modern computer technology in today's vehicles can navigate you to your destination, synchronize your cellular telephone to the on-board monitor for hands-free use and adjust radio and environmental controls by responding to voice-activated commands. The suspects' vehicles have increasingly become mobile storage places for evidence like the satellite navigation devices, laptops or storage media concealed from other household members. They also can hold other evidence linked to their travel for contact with like-minded adults and sexually exploited minors; like gasoline, toll booth and parking receipts or traffic tickets.

28. Prior to the advent of computers and the internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of images. To distribute these images on any scale also required significant resources. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computer technology and the Internet, producers, collectors and distributors of child pornography

can instantly and remotely upload images into virtual storage, like in the iCloud or Dropbox, allowing them to operate almost anonymously.

29. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, the development of computers (including cellular telephones) and wi-fi technology has also revolutionized the way in which those who seek child pornography are able to obtain this information. Computers, and the modern “smartphone,” allow simplified, often anonymous communication with persons far-removed from the solicitor. They can communicate with others with similar interests or where laws against sex with children are more lax or less enforced. They can also communicate directly with minor victims in a safe environment believing that their communications are anonymous. Computers also serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development and advancement of computers and internet technology has changed the methods used by those who seek to sexually exploit children and obtain access to child pornography in these ways.

30. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera, including cameras contained in the latest smartphones. A digital camera can be attached, using a device such as a cable, or digital images are often uploaded from the camera’s memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition,

there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

31. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as Comcast, AT&T and America Online (“AOL”), which allow subscribers to dial a local number or otherwise directly connect to a network, which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

32. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in sex with children or child pornography; and (ii) websites that offer images of child pornography. Like-minded individuals with a sexual interest in children and victims of child exploitation, as well as witnesses to online exploitation, can be identified through a person’s “contacts” lists, which may be termed in the form of “friends,” “contacts,” or “followers.” Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute or receive child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes, the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient’s computer, including the Internet history

and cache to look for “footprints” or “relics” of the websites and images accessed by the recipient.

33. The computer’s capability to store images in digital form makes it an ideal repository for child pornography. A single compact disk can store thousands of images and pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 500 gigabytes and larger are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the “scene of the crime.” Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

34. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is - in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more

recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

REQUEST FOR SEALING

35. It is respectfully requested that this Court issue an order sealing all papers submitted in support of this application, including the application and search warrant, for 180 days. I believe that sealing this document is necessary because the warrant identifies a known, juvenile victim of sexual exploitation. It is relevant to an ongoing investigation into the group of file-sharers, as not all the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through their various forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

36. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

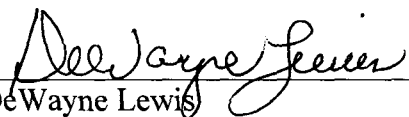
CONCLUSION

37. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Dropbox, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

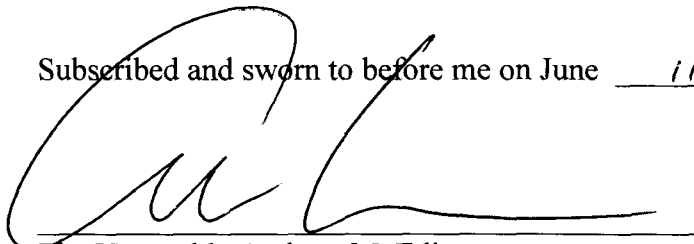
38. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction,” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Specifically, the Court “a district court of the United States . . . that – has jurisdiction over the offense being investigated.”

39. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,


DeWayne Lewis
Special Agent
DHS/ICE/Homeland Security Investigations

Subscribed and sworn to before me on June 11, 2018


The Honorable Andrew M. Edison
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with a Dropbox customer's account connected with the User ID: 912419232 and/or email address: malikberlanga2@gmail.com from the date of its creation through to the present that is stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., a company headquartered at 333 Brannon Street, San Francisco, California 94107.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Dropbox.com

To the extent that the information from the date of creation through to the present described herein is within the possession, custody, or control of Dropbox including any add/edit/delete logs, emails, records, files, other logs, or information that have been deleted but are still available to Dropbox, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox is required to disclose the following information to the government for each account or identifier listed:

- a. All other old or new accounts, with their contents and logs, utilized by the same customer.
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit card or bank account numbers);
- c. Log files
- d. The types of service utilized;
- e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. All records pertaining to communications between Dropbox, and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information from the date of creation through to the present described above that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, involving the customer's/user's account associated with **User ID: 912419232** and/or email address "**malikberlanga2@gmail.com**," including, for each account or identifier listed,

information pertaining to the following matters:

- a. All images depicting children engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256
- b. All electronic communications regarding children engaging in sexually explicit conduct;
- c. All communications with potential minors involving sexual topics or in an effort to seduce the minor.
- d. Any evidence that would tend to identify the person using the account when any of the items listed in subparagraphs a-c were sent, read, copied or downloaded.
- e. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

IV. Method of Delivery

Dropbox shall disclose items seized pursuant to this search warrant by sending (notwithstanding Title 18, United States Code, Section 2252A, or similar statute or code) to the listed Special Agent. Dropbox shall disclose responsive data, if any, by delivering on any digital media device via the United States Postal Service or commercial interstate carrier c/o Special Agent DeWayne Lewis, Homeland Security Investigations, 601 Rosenberg Avenue, Suite 201, Galveston, Texas 77550.